US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- December 2009 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for December 2009. It includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

Executive Summary

During December 2009, US-CERT issued 13 Current Activity entries, two (2) Technical Cyber Security Alerts, two (2) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include updates released by Adobe, Cisco, Hewlett-Packard, Microsoft, Mozilla, Research in Motion (RIM) Blackberry, Sun, and Apple; a malware campaign exploiting public interest in the H1NI virus; and a warning about Scareware pop-ups.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities currently being reported to US-CERT. The most significant entries of the month are highlighted below, followed by a table listing all of the entries posted this month.

Current Activity for December 2009	
December 1	Research In Motion Releases Advisory for BlackBerry PDF Distiller Vulnerabilities
December 2	H1N1 Malware Campaign Circulating
December 3	Microsoft Releases Advance Notification for December Security Bulletin
December 4	Sun Releases Update 17 for Java SE 6
December 8	Microsoft Releases December Security Bulletin
December 9	Adobe Releases Security Updates for Flash Player and AIR
December 11	Microsoft Releases Security Advisory 954157

Current Activity for December 2009	
December 11	HP Releases Update to Address OpenView Network Node Manager Vulnerabilities
December 14	FBI Releases Warning about Scareware
December 16	Mozilla Releases Firefox 3.5.6 and Firefox 3.0.16
December 16	Adobe Reader and Acrobat Remote Code Execution Vulnerability
December 17	Cisco Releases Security Advisory for Cisco WebEx WRF Player Vulnerabilities
December 22	Adobe Releases Security Update for Flash Media Server

- Adobe released updates for Adobe Reader, Acrobat, and Flash Media Player:
  - Adobe security advisory APSA09-07 addressed a vulnerability in Adobe Reader and Acrobat. By convincing a user to open a specially crafted PDF file, an attacker may be able to execute arbitrary code. Public reports currently indicate active exploitation of this vulnerability. Additional details can be found in US-CERT Vulnerability Note VU#508357.
  - Adobe security bulletin APSB09-18 addressed multiple vulnerabilities in Flash Media Server (FMS) 3.5.2 and earlier. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
- Cisco released security advisory cisco-sa-20091216-webex to address multiple vulnerabilities in WebEx Recording Format (WRF) Player. These vulnerabilities may allow an attacker to execute arbitrary code.
- HP released a security bulletin to address multiple vulnerabilities in OpenView Network Node Manager. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code. Review HP security bulletin c01950877 and apply any necessary updates to help mitigate the risks.
- Microsoft released updates for Microsoft Windows, Office, and Server:
  - The Microsoft Security Bulletin Summary for December 2009 addressed vulnerabilities in Microsoft Windows and Office. These vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
  - Security advisory 954157 was released to notify users of an update that increases the security of the Indeo codec on Microsoft Windows 2000, XP, and Server 2003. The advisory states that the Indeo codec running on these systems may allow remote code execution when opening specially crafted media content. Microsoft indicates that the update blocks the Indeo codec from being launched in Internet Explorer or Windows Media player, which removes a potential attack vector.
- Mozilla released Firefox 3.5.6 and Firefox 3.0.16 to address multiple vulnerabilities. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, operate with escalated privileges, or mislead users. These vulnerabilities may also affect SeaMonkey and Thunderbird.
- RIM released security advisory KB19860 to address multiple vulnerabilities in the PDF distiller of some released versions of the BlackBerry Attachment Service. The advisory lists the affected versions as BlackBerry Enterprise Server 5.0.0 running on Microsoft Windows version 2003 or 2008, BlackBerry Enterprise Server 5.0.0 running on Microsoft Windows 2000, BlackBerry Enterprise Server software versions 4.1.3 through 4.1.7, and BlackBerry Professional Software

4.1.4. By convincing a user to view a specially crafted PDF file, an attacker may be able to execute arbitrary code or cause a denial-of-service condition on the system that hosts the BlackBerry Attachment Service.

- Sun released update 17 for Java SE JDK 6 and Java SE JRE 6 to address multiple vulnerabilities. The impacts of these vulnerabilities include arbitrary code execution, privilege escalation, denial of service, and information disclosure. Additional details can be found in the Java SE 6 Update 17 release notes.
- Apple also released Java for Mac OS X 10.6 Update 1 and Java for Mac OS X 10.5 Update 6 to address these vulnerabilities. Mac users are encouraged to review Apple articles HT3969 and HT3970 and apply any necessary updates to help mitigate the risks.

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for December 2009	
December 8	TA09-342A Microsoft Updates for Multiple Vulnerabilities
December 9	TA09-343A Adobe Flash Vulnerabilities Affect Flash Player and Adobe AIR

Cyber Security Alerts

Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

Cyber Security Alerts (non-technical) for December 2009	
December 8	SA09-342A Microsoft Updates for Multiple Vulnerabilities
December 9	SA09-343A Adobe Flash Vulnerabilities Affect Flash Player and Adobe AIR

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for December 2009
SB09-341 Vulnerability Summary for the Week of November 30, 2009
SB09-348 Vulnerability Summary for the Week of December 7, 2009
SB09-355 Vulnerability Summary for the Week of December 14, 2009
SB09-362 Vulnerability Summary for the Week of December 21, 2009

A total of 436 vulnerabilities were recorded in the NVD during December 2009.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users. The December tips focused on denial-of-service attacks and spyware.

Cyber Security Tips for December 2009	
December 3	ST04-017 Protecting Portable Devices: Physical Security
December 17	ST04-018 Understanding Digital Signatures

Security Highlights

H1N1 Malware Campaign Circulating

US-CERT became aware of public reports of a malware campaign circulating via email messages offering information regarding the H1N1 vaccination. These email messages contained a link to a bogus Centers for Disease Control and Prevention website. Users who clicked on this link potentially became infected with malware. Public reports indicated that these email messages had subject lines such as: "Governmental registration program on the H1N1 vaccination" and "Your personal vaccination profile." Please note that subject lines may change at any time.

US-CERT encouraged users to take the following precautions to help mitigate the risks:

- Install antivirus software, and keep the signature files up to date.
- Do not follow unsolicited links, and do not open unsolicited email messages.
- Use caution when visiting untrusted websites.
- Refer to the Recognizing and Avoiding Email Scams (pdf) document for more information on avoiding email scams.
- Refer to the Avoiding Social Engineering and Phishing Attacks document for more information on avoiding social engineering attacks.

FBI Releases Warning about Scareware

The Federal Bureau of Investigation (FBI) released a warning to alert users about an ongoing threat involving pop-up security messages that appear on the Internet. These pop-up messages may have contained seemingly legitimate antivirus software. Users who clicked on these pop-up messages to purchase and install the bogus software potentially became infected with malicious code or were victims of a phishing attack.

US-CERT encouraged users and administrators to do the following to help mitigate the risks:

- Review the FBI Press Release titled Pop-Up Security Warnings Pose Threats.
- Install antivirus software, and keep the signature files up to date.
- Use caution when entering personal and financial information online.
- Install software applications from only trusted sources.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or to learn more about cyber security, please use one of the methods listed below. If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
Email Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xCB0CBD6E
PGP Key Fingerprint: 2A10 30D4 3083 2D28 032F 6DE3 3D60 3D81 CB0C BD6E
PGP Key: https://www.us-cert.gov/pgp/info.asc